In the claims:

All claims presented for examination are listed below.

~~Claim 1:~~ 1. (Currently amended) A method ~~and~~ ~~apparatus to secure~~ for a second operation of authenticating a user and securing an online ~~transactions~~ transaction over ~~the phone~~ a telephone, comprising:

(a) providing a card reader connecting a smart card to a telephone;

(b) [[-]]~~a smart card~~ transmitting [[a]] from the smart card at least an identification sequence for the user to an IVR server connected to a telephone line in the form of a modulated signal[[,]];

~~-a card reader plugged into the telephone line,~~

[[-]] (c) ~~an IVR applet~~ demodulating the identification sequence at the IVR server, and

(d) authenticating the user and the transaction at an application server receiving the demodulated identification sequence from the IVR server over a communication network wherein data processing required for generating, transmitting and authenticating the user occur without data processing assistance from ~~characterized by the absence of processing means within~~ the card reader.

~~Claim 2: A~~ 2. (Currently amended) The method [[as in]] of claim 1, wherein the identification sequence comprises at least a unique card number and a random number, the random number valid only once.

~~Claim 3: A~~ 3. (Currently amended) The method as in claim 2, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

~~Claim 4: A~~ 4. (Currently amended) The method as in claim 3, wherein the session key (Ki) is a function of [[the]] a previous one (Ki-l) emitted by the card ~~such~~ as: Ki G(Ki-l), G is a one-way function ~~also~~ wherein (Ki-1) is known by the authentication server.

~~Claim 5: A~~ 5. (Currently amended) The method ~~as in~~ of claim 4, wherein the session key (Ki) is used by the IVR applet to encrypt [[the]] a PIN entered by the user; ~~said~~ wherein an encryption code is transmitted to the authentication server along with the card number.

~~Claim 6: A~~ 6. (Currently amended) The method ~~as in~~ of claim 5, wherein the authentication server decrypts the encryption code to retrieve the user PIN, using a session key deduced from the ~~previous one~~ (Ki-l) stored in [[the]] a database at the authentication server ~~database~~.

~~Claim 7: A~~ 7. (Currently amended) The method ~~as in~~ of claim 6, wherein the authentication is valid only if the decrypted PIN and the PIN stored in the database are identical; if this is the case, the authentication server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.

8-13. (Canceled)

14. (New) A system for authenticating a user and securing online transactions for a user over a telephone, comprising;

a card reader connected to the telephone and the telephone connected to a telephone line;

a smart card connected to the card reader for transmitting at least an identification sequence for the user;

an IVR server connected to the telephone line; and

an application server connected to the IVR server over a communication network;

wherein the system authenticates the user and the online transactions by the application server which receives the demodulated identification sequence from the IVR server over a communication network and compares the received identification sequence with identification information in database accessible to the user and all of the data processing required to transmit information and authenticate the user occurs outside of the card reader.

15. (New) The system of claim 14, wherein the identification sequence comprises at least a unique card number and a random number valid only once.

16. (New) The system of claim 14, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

17. (New) The system of claim 14, wherein the session key (Ki) is a function of a previous one (Ki-l) emitted by the card such as: Ki G(Ki-l), G is a one-way function, wherein (Ki-1) is known by the authentication server.

18. (New) The system of claim 14, wherein the session key (Ki) is used by the IVR applet to encrypt a PIN entered by the user; said encryption code is transmitted to the authentication server along with the card number.

19. (New) The system of claim 14, wherein the authentication server decrypts the encryption code to retrieve the user PIN, using a session key deduced from the previous one (Ki-l) stored in a database at the authentication server.

20. (New) The system of claim 14, wherein the authentication is valid only if the decrypted PIN and the PIN stored in the database are identical; if this is the case, the authentication server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.

21. (New) The system of claim 14, wherein the smart card is powered by the voltage provided by the telephone line.

22. (New) The system of claim 14, wherein the smart card transmits the modulated signal to the telephone line through an ISO contact.

23. (New) The system of claim 14, wherein the card reader is further integrated into the telephone handset.